

[COMPANY LETTERHEAD]

[DATE]

[INDIVIDUAL NAME]

[STREET ADDRESS]

[CITY, STATE AND POSTAL CODE]

Re: April 21, 2021 Cybersecurity Incident

Dear [INDIVIDUAL NAME]:

We value you and respect the privacy of your information, which is why, as a precautionary measure, we are writing to provide you with more information about the data security incident that took place on April 21, 2021, and to inform you that the incident may involve your personal information and provide you with additional steps you can take to protect yourself.

On April 21, 2021, we learned that early that morning an unidentified third party logged into several of our servers and eight windows desktop computers and installed ransomware. Ransomware is a form of computer virus that locks computer files preventing access to the information. Although a review of our network logs show that the data we received during the incident was approximately the size of the computer virus files installed, and only a small amount of information was received by the third-party (~30mb, which was likely the amount necessary to maintain the connection and set up the ransomware), we are unable to definitively rule out that no confidential information was taken from the computer systems. The data contained on the affected systems included personal information such as:

First Name

Last Name

Physical Address

Social Security Number

Driver's License Numbers

Bank Account Numbers

Medical Records

Farmingdale Meat Market ("FMM") values your privacy and deeply regrets that this incident occurred. FMM has conducted a thorough review of the potentially affected computer systems, and has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of FMM's valued employees, including but not limited to: implementing multi-factor authentication for all VPN users, installing an advanced anti-virus and anti-malware solution, providing cybersecurity awareness training to all employees, and providing you, and all other affected employees, with identity theft protection through Norton LifeLock ("LifeLock") for the next two years.

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information, and if you have not signed up already, how to sign up for identity theft protection for the next two years.

For further information and assistance, please contact [NAME OF COMPANY REPRESENTATIVE] at [TELEPHONE NUMBER/TOLL-FREE NUMBER] between [TIME] a.m.- [TIME] p.m. [EST] daily.

Sincerely,

[NAME]

[TITLE]

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834
---	--	--

Fraud Alert

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at [http:// www.annualcreditreport.com](http://www.annualcreditreport.com).

Identify Theft Protection Through LifeLock

In addition, FMM has arranged with LifeLock to provide you with identify theft protection for two years, at no cost to you. The LifeLock Defender™ Preferred package provides you with the following benefits:

- Primary Identity Alert System
- 24/7 Live Member Support
- Dark Web Monitoring
- Norton™ Security Deluxe² (90 Day Free Subscription)
- Stolen Funds Reimbursement up to \$25,000
- Personal Expense Compensation up to \$25,000
- Coverage for Lawyers and Experts up to \$1 million
- U.S.-based Identity Restoration Team
- Annual Three-Bureau Credit Reports & Credit Scores
- Three-Bureau Credit Monitoring¹
- USPS Address Change Verification Notifications
- Fictitious Identity Monitoring
- Credit, Checking and Savings Account Activity Alerts

Please see the descriptions on the signup page, and lifelock.com for a complete explanation of the benefits provided by the LifeLock Defender™ Preferred package

To take advantage of this offer, you must enroll before June 30, 2021.

To activate your membership online and get protection at no cost to you:

1. You will need the following **Promo Code:** DCWHLMT2104 and **Member ID:** [MEMBER ID NUMBER], which have been assigned specifically to you, for one-time use.
2. To begin, please click on the following URL:
[https://www.lifelock.com/store?promocode=DCWHLMT2104&inid=hp-csp_false&memberid=\[MEMBER ID NUMBER\]](https://www.lifelock.com/store?promocode=DCWHLMT2104&inid=hp-csp_false&memberid=[MEMBER ID NUMBER])
3. Your complimentary offer is presented. Click the red “START YOUR MEMBERSHIP” button.
4. Once enrollment is completed, you will receive a confirmation email (be sure to follow ALL directions in this email).

Alternatively, to activate your membership over the phone, please call: 1-800-899-0180

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors

from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338).

You may wish to review the tips provided by your local state agencies on how to protect yourself. For more information, please visit the following sites or call the following numbers:

- **New York Attorney General**
<https://ag.ny.gov/internet/privacy-and-identity-theft>
1-800-771-7755
- **Vermont Attorney General**
<https://ago.vermont.gov/identity-theft/>
(802) 828-3171